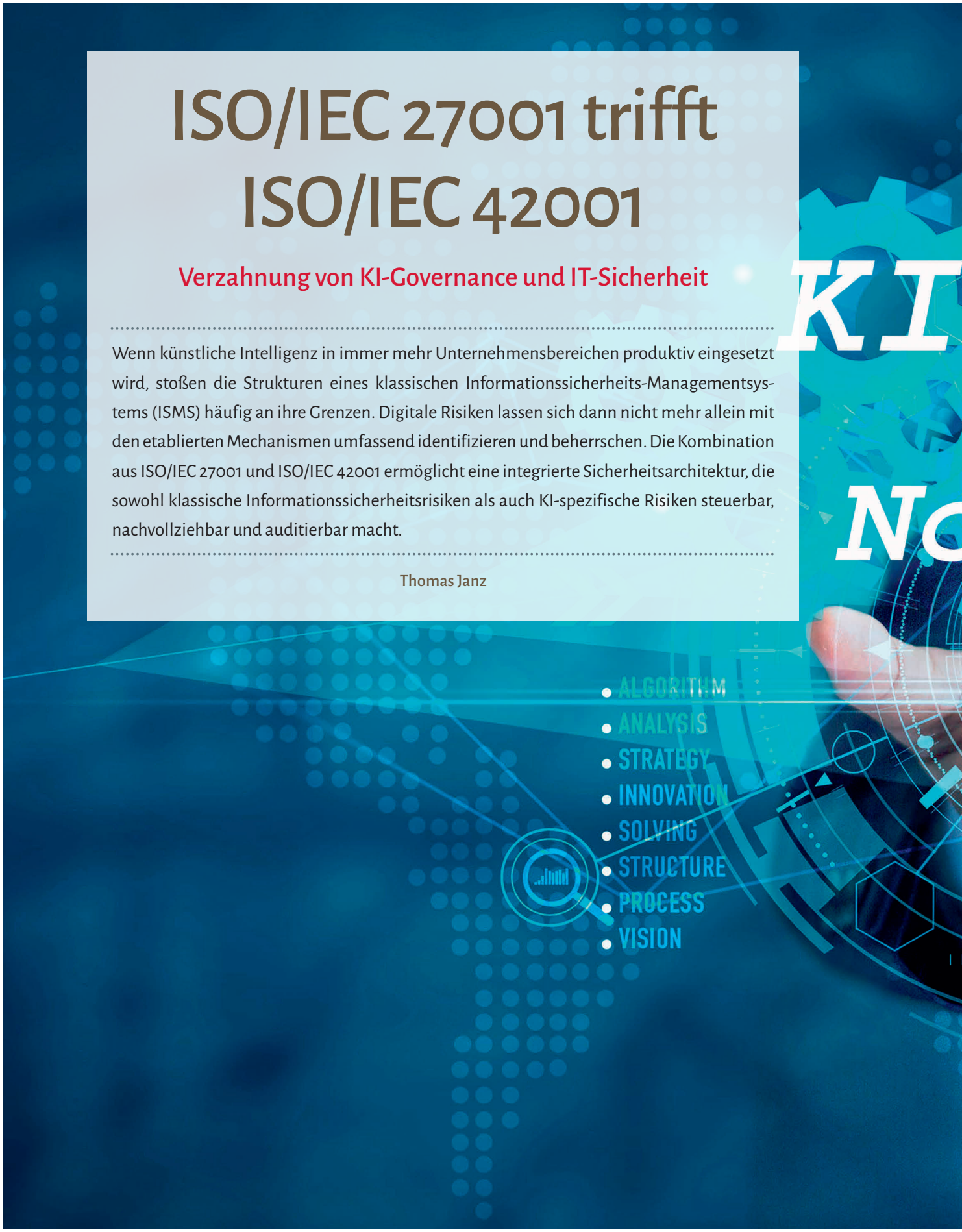
ISO/IEC 27001 trifft ISO/IEC 42001

Verzahnung von KI-Governance und IT-Sicherheit

Wenn künstliche Intelligenz in immer mehr Unternehmensbereichen produktiv eingesetzt wird, stoßen die Strukturen eines klassischen Informationssicherheits-Managementsystems (ISMS) häufig an ihre Grenzen. Digitale Risiken lassen sich dann nicht mehr allein mit den etablierten Mechanismen umfassend identifizieren und beherrschen. Die Kombination aus ISO/IEC 27001 und ISO/IEC 42001 ermöglicht eine integrierte Sicherheitsarchitektur, die sowohl klassische Informationssicherheitsrisiken als auch KI-spezifische Risiken steuerbar, nachvollziehbar und auditierbar macht.

Thomas Janz



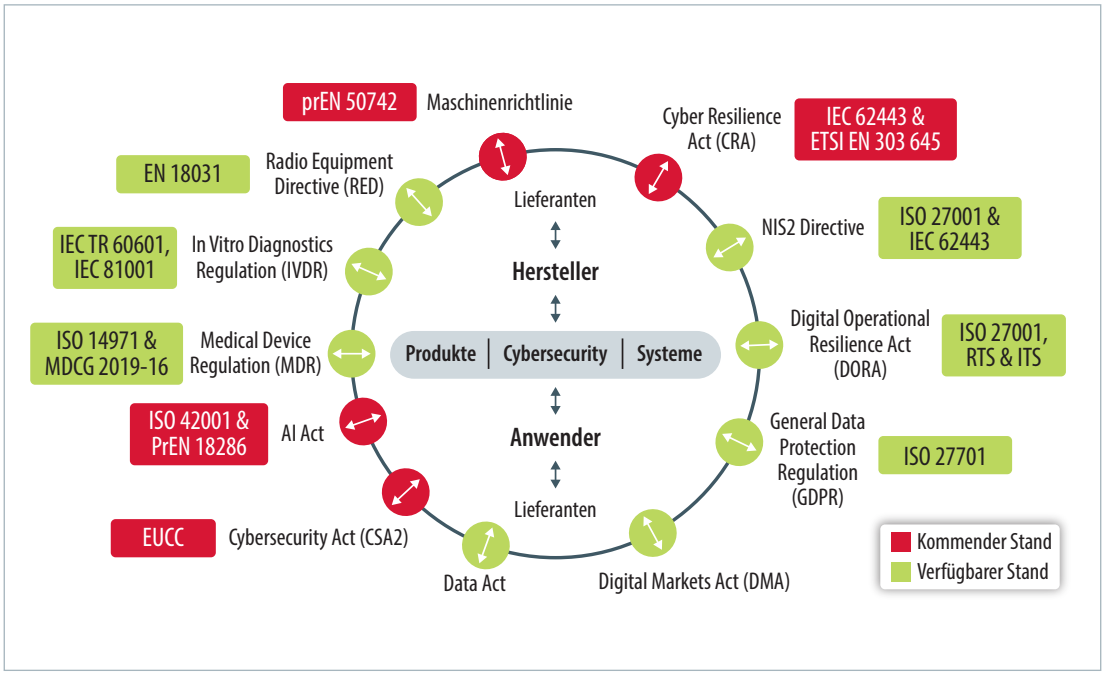
Künstliche Intelligenz ist in vielen Organisationen längst keine experimentelle Technologie mehr. In der Energieversorgung werden beispielsweise KI-basierte Analysen zur Steuerung und Stabilisierung von Stromnetzen eingesetzt. Fehlerhafte Entscheidungen können hier zu Instabilitäten im Netzbetrieb, Versorgungsengpässen oder im Extremfall zu Blackouts führen. Auch in anderen Bereichen wird KI mehr und mehr zum Bestandteil geschäfts- und sicherheitskritischer Prozesse.

Vor diesem Hintergrund steigen die Anforderungen an Steuerbarkeit, Nachvollziehbarkeit und Governance deutlich. Gleichzeitig bleibt die Gefahr, dass Unternehmen Ziel eines Cyberangriffs werden, unverändert hoch. Eine integrierte Betrachtung von Informationssicherheit und KI-Governance wird damit zu einem zentralen Erfolgsfaktor.

Tech-Regulierung in volatilen Zeiten

Entsprechend entwickeln sich auch die regulatorischen Rahmenbedingungen weiter, um die fortschreitende Digitalisierung zu lenken. Mit der EU KI-Verordnung (EU AI Act) ist erstmals ein umfassender Rechtsrahmen für die Entwicklung, den Einsatz und den Betrieb Künstlicher Intelligenz geschaffen worden. Auch wenn aktuell einzelne Aspekte – etwa die mögliche Herauslösung bestimmter Hochrisiko-Produktbereiche im Rahmen des sogenannten digitalen EU-Omnibus – diskutiert werden, ist davon auszugehen, dass für viele Geschäftsfelder verbindliche regulatorische Anforderungen im Umgang mit KI gelten werden.

Gleichzeitig verfolgt die europäische Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-2) das Ziel, ein einheitlich hohes IT-Sicherheitsniveau in allen EU-Mitgliedstaaten zu etablieren. Im Fokus stehen dabei die Cybersicherheit von Netzwerken und Informationssystemen sowie verbindliche Anforderungen an ein strukturiertes Risikomanagement, die Einführung eines Informationssicherheits-Managementsystems (ISMS) und die Absicherung von Lieferketten. Weitere Regelwerke auf europäischer Ebene, etwa der EU Data Act oder der Cyber Resilience Act, »»



Die EU reguliert Cybersecurity mittels unterschiedlicher gesetzlicher Vorgaben. Internationale Standards wie ISO 27001 oder ISO 42001 helfen bei ihrer Umsetzung.

© Tüv Süd

sowie nationale Gesetze wie das IT-Sicherheitsgesetz oder branchenspezifische Vorgaben ergänzen diesen regulatorischen Rahmen.

Für Qualitäts-, Sicherheits- und Managementverantwortliche stellt sich damit eine zentrale Frage: Reicht ein etabliertes ISMS nach ISO/IEC 27001 aus, um auch KI-basierte Systeme sicher und rechtskonform zu betreiben, oder ist ergänzend ein KI-Managementsystem nach ISO/IEC 42001 erforderlich?

ISO/IEC 27001: Stabiles Fundament mit klaren Grenzen

ISO/IEC 27001 („Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme – Anforderungen“) bietet Organisationen eine strukturierte Vorgehensweise zur Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Die Norm unterstützt Organisationen dabei, Resilienz, Compliance und Cybersicherheit systematisch zu stärken. Eine Zertifizierung dient als relevanter Nachweis gegenüber Kunden, Partnern und Aufsichtsbehörden, dass ein definiertes und angemessenes Sicherheitsniveau erreicht ist.

Die Norm fokussiert auf Informationen, Systeme und Prozesse. KIspezifische Fragestellungen – etwa zur Qualität von Trainingsdaten, zum Verhalten von Modellen oder zu möglichen Bias-Effekten – werden nur mittelbar adressiert. Sobald KI jedoch entscheidungsrelevant eingesetzt wird, kann daraus eine Governance-Lücke entstehen, die mit den klassischen ISMS-Mechanismen allein nicht vollständig geschlossen werden kann.

ISO/IEC 42001: KI-Governance als Ergänzung zum ISMS

ISO/IEC 42001 („Informationstechnik - Künstliche Intelligenz – Managementsystem“) schließt diese Lücke, indem sie Anforderungen an ein Artificial Intelligence Management System (AIMS) für Organisationen definiert, die KI-Systeme entwickeln, bereitstellen oder nutzen. Die Norm adressiert Risiken aus Entwicklung, Training, Bereitstellung und Betrieb von KI-Systemen – darunter etwa Fehlentscheidungen, Bias, Modelldrift oder Systemausfälle – und fordert dafür Governance-Strukturen mit klar definierten Rollen und Verantwortlichkeiten.

Zentrale Elemente sind ein KI-spezifisches Risikomanagement, Anforderungen an Transparenz und Verständlichkeit, eine durchgängige Dokumentation über den gesamten KI-Lebenszyklus sowie kontinuierliches Monitoring und regelmäßige Reviews. Für kritische Entscheidungsprozesse verankert die ISO/IEC 42001 zudem Konzepte menschlicher Aufsicht („Human-in-the-Loop“ bzw. „Human Oversight“).

Ein Managementsystem nach ISO/IEC 42001 ermöglicht Organisationen algorithmische Risiken, Bias-Effekte, Fehlentscheidungen und Systemausfälle systematisch zu steuern und KI-Systeme transparent, erklärbar und auditierbar zu gestalten.

Ein gemeinsamer Ansatz statt doppelter Strukturen

Der größte Mehrwert für resiliente und vertrauenswürdige digitale Systeme entsteht nicht durch parallele Managementsysteme, sondern durch deren konsequente Integration. Sowohl ISO/IEC 27001 als auch ISO/IEC 42001 basieren auf der von der ISO definierten High Level Structure (HLS) für Managementsystemnormen und folgen dem Plan-Do-Check-Act (PDCA) -Zyklus. Dadurch lassen sich ein integriertes Informationssicherheits und KI-Managementsystem (ISMS/AIMS) ohne redundante Prozesse und Doppelstrukturen aufbauen.

Ein integriertes Risiko und Governance-Modell schafft ein einheitliches Verständnis für klassische Informationssicherheits- und KI-Risiken. Anstelle getrennter Risikoregister werden Risikoanalysen konsolidiert und Rollenmodelle zwischen Informationssicherheit und KI-Verantwortung aufeinander abgestimmt. Dadurch lassen sich Datenverluste minimieren, Sicherheitsvorfälle schneller bewältigen und gesetzliche sowie branchenspezifische Anforderungen konsistent erfüllen.

In der praktischen Umsetzung sind jedoch Integrationshürden zu berücksichtigen. Während die ISO/IEC 27001 seit vielen

Jahren etabliert ist und auf umfangreiche Best Practices sowie eine breite Anwender- und Audit-Community zurückgreifen kann, ist die ISO/IEC 42001 noch vergleichsweise jung. Die Norm wurde Ende 2023 veröffentlicht, weshalb bislang weniger Erfahrungswerte, spezialisierte Werkzeuge und Auditoren mit entsprechender Expertise verfügbar sind.

Auch operativ ergeben sich bei der Integration beider Managementsysteme spezifische Herausforderungen:

- **Governance:** Beide Normen verlangen klar definierte Rollen und Verantwortlichkeiten, setzen jedoch unterschiedliche Schwerpunkte. Dies kann zu Überschneidungen oder Unklarheiten führen – etwa bei der Frage, wer für die Risikobewertung von KI-Systemen verantwortlich ist: der Informationssicherheitsbeauftragte oder ein KI-Ethik-Gremium. Eine erfolgreiche Integration erfordert daher ein klares Verständnis der Schnittstellen zwischen Informationssicherheit und ethischen KI-Prinzipien.
- **Risikomanagement:** ISO/IEC 27001 fordert ein Informationssicherheits-Risikomanagement entlang der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. ISO/IEC 42001 ergänzt dies um ein KI-spezifisches Risikomanagement, das auch gesellschaftliche, ethische und rechtliche Risiken berücksichtigt. Um Redundanzen zu vermeiden und Synergien zu nutzen, sollten beide Ansätze in einem integrierten Risikomanagement zusammengeführt werden.
- **Dokumentation und Nachweisführung:** Beide Normen verlangen eine umfassende Dokumentation, etwa von Richtlinien, Verfahren und Risikoanalysen. Unterschiedliche Anforderungen an Transparenz und Nachvollziehbarkeit – insbesondere bei Entscheidungen durch KI-Systeme – können den Dokumentationsaufwand erhöhen und müssen gezielt harmonisiert werden.
- **Technologische Komplexität:** KI-Systeme bringen zusätzliche technische Herausforderungen mit sich, etwa Black-Box-Modelle, Anforderungen an Datenqualität oder den Umgang mit Bias. Diese Aspekte müssen in bestehende Sicherheitsarchitekturen integriert werden und erfordern zusätzliche Kompetenzen sowie spezialisierte Ressourcen.
- **Kulturelle und organisatorische Aspekte:** Die Einführung eines KI-Managementsystems geht häufig mit einem Kulturwandel einher, insbesondere im Hinblick auf ethische Fragestellungen und Verantwortlichkeiten. In Kombination mit einem bestehenden ISMS kann dies zu Widerständen oder Überforderung führen, wenn kein begleitendes Change-Management erfolgt.

Praxis: Drei Hebel für resiliente und vertrauenswürdige digitale Systeme

Um die beschriebenen Herausforderungen zu adressieren, haben sich in der Praxis drei zentrale Erfolgsfaktoren für integrierte Managementsysteme nach ISO/IEC 27001 und ISO/IEC 42001 herauskristallisiert:

- **Sicherheits- und Vertrauensarchitektur als Fundament:** Eine ganzheitliche Sicherheitsarchitektur verbindet klassische Informationssicherheitsmaßnahmen, wie Schutzbedarfsfeststellungen, Zugriffskontrollen und Logging, mit KI-spezifischen Kontrollen wie Nachweisen zu Datenherkunft, formalen Modellfreigaben oder der Erkennung von Modelldrift. Ziel ist es, KI-gestützte Prozesse belastbar abzusichern und Vertrauen in deren Ergebnisse zu schaffen.
- **Governance Strukturen verzahnen:** Ein gemeinsames Governance Board oder ein erweitertes ISMS-Gremium schafft Verbindlichkeit über Domänengrenzen hinweg. Es definiert Rollen, Entscheidungsbefugnisse und Eskalationswege, konsolidiert Richtlinien zu Daten, Modellen oder Lieferanten und verhindert Silobildung zwischen Security, IT, Data-/AI-Funktionen und Fachbereichen.
- **Transparenz und Nachvollziehbarkeit operationalisieren:** Für den Einsatz von KI in geschäfts- oder sicherheitskritischen Prozessen sollten Audit Trails, technische Nachweise und definierte Review-Zyklen zum Standard gehören. Dazu zählen unter anderem Modell- und Datendokumentationen, erklärbare Ausgaben (Explainable AI, wo sinnvoll), ein kontinuierliches Monitoring von Qualität, Drift und Fehlerraten sowie klar definierte Kriterien für menschliche Eingriffe oder Übersteuerungen.

Sinnvoll: Verzahnung von ISO/IEC 27001 und ISO/IEC 42001

ISO/IEC 27001 bleibt das Fundament einer wirksamen Informationssicherheit. Sobald Organisationen jedoch KI-Systeme entwickeln, betreiben oder KI-basierte Entscheidungen in geschäfts- oder sicherheitskritische Prozesse integrieren, rücken zusätzliche Risiko-Dimensionen in den Fokus – etwa Modelldrift, Bias oder eine fehlende Nachvollziehbarkeit algorithmischer Entscheidungen. Diese Aspekte werden von einem klassischen ISMS nur indirekt adressiert. ISO/IEC 42001 ergänzt diesen Ansatz durch KI-spezifische Governance-Strukturen, Rollenmodelle und Nachweisanforderungen. Integriert umgesetzt entsteht eine verzahnte Governance, die Informations- und KI-Risiken in einer konsolidierten Steuerung zusammenführt und Verantwortlichkeiten klar strukturiert.

Auch wenn eine Zertifizierung nach ISO/IEC 27001 und ISO/IEC 42001 für sich genommen keine automatische Rechtskonformität garantiert, bieten beide Standards einen anerkannten und auditierbaren Rahmen für eine systematische Governance. Auf dieser Basis lassen sich Anforderungen aus dem EU AI Act und der NIS-2-Richtlinie strukturiert in ein integriertes Managementsystem überführen und gegenüber Kunden, Partnern und Aufsichtsbehörden nachvollziehbar nachweisen. Entsprechend weist das Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hin, dass eine ISO/IEC 27001-Zertifizierung keine NIS-2-Konformität ersetzt, jedoch eine belastbare Grundlage für deren Umsetzung darstellt. ■

INFORMATION & SERVICE

AUTOR

Thomas Janz ist Product Compliance Manager IT-Standards bei TÜV SÜD.

KONTAKT

TÜV SÜD Management Service GmbH
Ridlerstr. 57
80339 München
thomas.janz@tuvsud.com
www.tuvsud.com/tms